

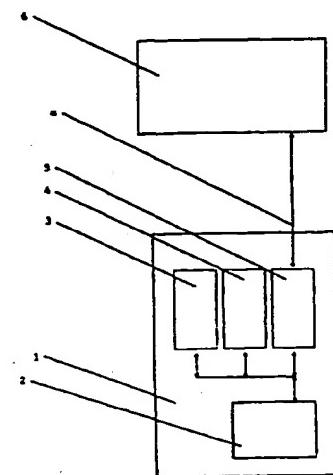
PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM  
Internationales Büro



INTERNATIONALE ANMELDUNG VERÖFFENTLICH NACH DEM VERTRAG ÜBER DIE  
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation <sup>6</sup> : <b>H04L 9/08</b>		A1	(11) Internationale Veröffentlichungsnummer: <b>WO 95/34968</b>
			(43) Internationales Veröffentlichungsdatum: <b>21. December 1995 (21.12.95)</b>
(21) Internationales Aktenzeichen: <b>PCT/DE95/00733</b>			(81) Bestimmungsstaaten: AU, BR, CN, CZ, JP, KR, NO, PL, RU, SG, US, europäisches Patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
(22) Internationales Anmeldedatum: <b>30. Mai 1995 (30.05.95)</b>			
(30) Prioritätsdaten: <b>P 44 20 970.3 16. Juni 1994 (16.06.94) DE</b>			<b>Veröffentlicht</b> <i>Mit internationalem Recherchenbericht. Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist. Veröffentlichung wird wiederholt falls Änderungen eintreffen.</i>
(71) Anmelder ( <i>für alle Bestimmungsstaaten ausser US</i> ): <b>ESD VERMÖGENSVERWALTUNGSGESELLSCHAFT MBH [DE/DE]; Briener Strasse 10, D-80333 München (DE)</b>			
(72) Erfinder; und			
(75) Erfinder/Anmelder ( <i>nur für US</i> ): <b>BUGOVICS, Jozsef [HU/DE]; Kreuzstrasse 11, D-06886 Lutherstadt Wittenberg (DE)</b>			
(74) Anwalt: <b>HAUSSINGEN, Peter; Franz-Heymann-Strasse 70, D-06526 Sangerhausen (DE)</b>			
(54) Title: <b>DEVICE FOR DECODING DECODING ALGORITHMS AND METHOD OF ENCRYPTING AND DECODING SUCH ALGORITHMS USING THE DEVICE</b>			
(54) Bezeichnung: <b>ENTSCHLÜSSELUNGSEINRICHTUNG VON ENTSCHEIDUNGSEALGORITMEN UND VERFAHREN ZUR DURCHFÜHRUNG DER VER- UND ENTSCHEIDUNG DERSELBEN</b>			
(57) Abstract			
<p>The aim of the invention is to develop a system and method which can work with variable encryption algorithms and which ensures the secure transfer of the algorithm without it being detected and prevents the algorithm without it being detected and prevents the algorithm being broken. This aim is achieved by virtue of the fact that the decoding device consists of an integrated circuit (1) associated with a central processing unit (2), an internal non-readable volatile random-access memory (3) used as working memory and an internal non-readable non-volatile read-only memory (4) plus an interface (5), each decoding device differing from every other by the content of the ROM (4) and being partly integrated in an integrated circuit (1) and that the interface (5) is located between the central processing unit (2) and the personal computer (6) and connected, together with central processing unit (2), to the personal computer (6) by a data path (a).</p>			
(57) Zusammenfassung			
<p>Die Erfindung betrifft eine Entschlüsselungseinrichtung von Entschlüsselungsalgorithmen und Verfahren zur Durchführung der Ver- und Entschlüsselung derselben. Die Aufgabe ist es, eine Vorrichtung und ein Verfahren als System zu entwickeln, welches mit variablen Verschlüsselungsalgorithmen arbeiten kann und die Übertragung des Verschlüsselungsalgorithmus gegen Erkennen sichert und das Brechen des Verschlüsselungsalgorithmus verhindert. Erfindungsgemäß wird die Aufgabe dadurch gelöst, daß die Entschlüsselungseinrichtung aus einem integrierten Schaltkreis (1), dem ein Zentralprozessor CPU (2), ein interner nichtauslesbarer flüchtiger Speicher mit wahlfreiem Zugriff RAM (3) als Arbeitsspeicher und ein interner nichtauslesbarer nichtflüchtiger Speicher mit wahlfreiem Zugriff ROM (4) und einem Interface (5) zugeordnet sind, indem sich jede Entschlüsselungseinrichtung von jeder weiteren unterscheidet durch den Inhalt des internen nichtflüchtigen Speichers mit wahlfreiem Zugriff ROM (4) und teilweise in einem integrierten Schaltkreis integriert ist und daß das Interface (5) zwischen dem Zentralprozessor CPU (2) und dem Personalcomputer (6) angeordnet ist und mit dem Zentralprozessor CPU (2) mit dem Datenpfad (a) verbunden sind.</p>			



#### ***LEDIGLICH ZUR INFORMATION***

**Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.**

<b>AT</b>	<b>Österreich</b>	<b>GA</b>	<b>Gabon</b>	<b>MR</b>	<b>Mauretanien</b>
<b>AU</b>	<b>Australien</b>	<b>GB</b>	<b>Vereinigtes Königreich</b>	<b>MW</b>	<b>Malawi</b>
<b>BB</b>	<b>Barbados</b>	<b>GE</b>	<b>Georgien</b>	<b>NE</b>	<b>Niger</b>
<b>BE</b>	<b>Belgien</b>	<b>GN</b>	<b>Guinea</b>	<b>NL</b>	<b>Niederlande</b>
<b>BF</b>	<b>Burkina Faso</b>	<b>GR</b>	<b>Griechenland</b>	<b>NO</b>	<b>Norwegen</b>
<b>BG</b>	<b>Bulgarien</b>	<b>HU</b>	<b>Ungarn</b>	<b>NZ</b>	<b>Neuseeland</b>
<b>BJ</b>	<b>Benin</b>	<b>IE</b>	<b>Irland</b>	<b>PL</b>	<b>Polen</b>
<b>BR</b>	<b>Brasilien</b>	<b>IT</b>	<b>Italien</b>	<b>PT</b>	<b>Portugal</b>
<b>BY</b>	<b>Belarus</b>	<b>JP</b>	<b>Japan</b>	<b>RO</b>	<b>Rumänien</b>
<b>CA</b>	<b>Kanada</b>	<b>KE</b>	<b>Kenya</b>	<b>RU</b>	<b>Russische Föderation</b>
<b>CF</b>	<b>Zentrale Afrikanische Republik</b>	<b>KG</b>	<b>Kirgisistan</b>	<b>SD</b>	<b>Sudan</b>
<b>CG</b>	<b>Kongo</b>	<b>KP</b>	<b>Demokratische Volksrepublik Korea</b>	<b>SE</b>	<b>Schweden</b>
<b>CH</b>	<b>Schweiz</b>	<b>KR</b>	<b>Republik Korea</b>	<b>SI</b>	<b>Slowenien</b>
<b>CI</b>	<b>Côte d'Ivoire</b>	<b>KZ</b>	<b>Kasachstan</b>	<b>SK</b>	<b>Slowakei</b>
<b>CM</b>	<b>Kamerun</b>	<b>LI</b>	<b>Liechtenstein</b>	<b>SN</b>	<b>Senegal</b>
<b>CN</b>	<b>China</b>	<b>LK</b>	<b>Sri Lanka</b>	<b>TD</b>	<b>Tschad</b>
<b>CS</b>	<b>Tschechoslowakei</b>	<b>LU</b>	<b>Luxemburg</b>	<b>TG</b>	<b>Togo</b>
<b>CZ</b>	<b>Tschechische Republik</b>	<b>LV</b>	<b>Lettland</b>	<b>TJ</b>	<b>Tadschikistan</b>
<b>DE</b>	<b>Deutschland</b>	<b>MC</b>	<b>Monaco</b>	<b>TT</b>	<b>Trinidad und Tobago</b>
<b>DK</b>	<b>Dänemark</b>	<b>MD</b>	<b>Republik Moldau</b>	<b>UA</b>	<b>Ukraine</b>
<b>ES</b>	<b>Spanien</b>	<b>MG</b>	<b>Madagaskar</b>	<b>US</b>	<b>Vereinigte Staaten von Amerika</b>
<b>FI</b>	<b>Finnland</b>	<b>ML</b>	<b>Mali</b>	<b>UZ</b>	<b>Usbekistan</b>
<b>FR</b>	<b>Frankreich</b>	<b>MN</b>	<b>Mongolei</b>	<b>VN</b>	<b>Vietnam</b>

Entschlüsselungseinrichtung von Entschlüsselungsalgorithmen und Verfahren zur Durchführung der Ver- und Entschlüsselung derselben

Die Erfindung betrifft eine Entschlüsselungseinrichtung von Entschlüsselungs-algorithmen und das Verfahren zur Durchführung der Ver- und Entschlüsselung derselben, indem die Entschlüsselungseinrichtung Berechtigten den Zugriff gewährt und Unberechtigte vom Zugriff ausschließt.

Digitale Informationen werden in immer größerem Maßstab über gesicherte Verteilungskanäle versandt. Diese Informationen sollen aber nur bestimmte Empfänger erreichen und nicht von Unbefugten gelesen werden können. Die Prozeduren zur Übertragung von solchen Informationen sind heute schon sehr an die Bedürfnisse der Industrie angepaßt.

Die weitere Entwicklung der Rechentechnik zeigt aber Probleme bei der Sicherheit der gegenwärtig verwendeten Ver-/ Entschlüsselungsalgorithmen auf.

Ein Verschlüsselungsalgorithmus der zur Zeit vorrangig von der Industrie verwendet wird, ist der „data-encryption algorithm“ DEA, der von IBM seit 1960 entwickelt und 1977 vom U.S. National Bureau of Standards zur Norm erklärt wurde.

Dieser Verschlüsselungsalgorithmus ist zur Zeit in der Prüfung zur deutschen und internationalen Normung.

Es hat immer wieder Versuche zur Entschlüsselung von mit dem DEA verschlüsselten Informationen Gegeben. Diese waren bisher nach dem Stand der Technik (da die Rechenleistungen nicht zur Verfügung standen) nicht erfolgreich.

Es wurden jedoch in jüngster Zeit Spezialprozessoren entwickelt, welche speziell zur Entschlüsselung von Verschlüsselungssystemen geeignet sind. Damit ist es z. B. möglich, den Standard DEA zu brechen (mit Hardwarekosten von ca. 80000 \$,

Stand 1992). Einen guten Überblick über die Entwicklung gibt Richard Zippel, in „Programming the Data structure accelerator“ in Proceedings of Jerusalem Conference of Information, Technology, Jerusalem, Israel, October 1990.

5 Damit kommt der Entwicklung und Verwendung von neuen Verschlüsselungsalgorithmen große Bedeutung zu.

Da es aber nicht möglich ist, einen sicheren Verschlüsselungsalgorithmus zu entwickeln, ist es notwendig, eine Austauschbarkeit der Algorithmen zu ermöglichen.

10 Die modernen Möglichkeiten zum Brechen eines Verschlüsselungsalgorithmus beruhen auf dem Vorhandensein von sogenannten Plaintexten (unverschlüsselte Informationen) und der dazugehörigen Ciphertexte (verschlüsselte Information). Um Blocksysteme, wie z. B. den DEA zu brechen, muß die Menge diese Texte sehr groß sein. Dies ist z. B. notwendig, um solche Methoden, wie die differentielle 15 Cryptoanalyse von Biham und Shamir, durchzuführen. Diese Methode ist der beste zur Zeit bestehende Angriff auf Blockverschlüsselsysteme wie den DEA (beschrieben in Eli Biham und Adi Shamir „Differential Cryptoanalysis of DES-like Cryptosystems“ in Journal of Cryptology vol. 4 pp 3-72, 1991).

20 Es ist also nötig, die Menge der Dritten zur Verfügung stehenden Plain-/Ciphertexte möglichst gering zu halten. Dies ist möglich, wenn die Informationen mit öfter wechselnden Verschlüsselungsalgorithmen verschlüsselt werden. Dritte, welche die Nachrichten entschlüsseln wollen, müssen dann jedesmal einen neuen „Knackalgorithmus“ entwickeln, wenn das Verschlüsselungsverfahren gewechselt wird.

25 Es ist folglich nötig, ein System zu schaffen, welches mit variablen Verschlüsselungsalgorithmen arbeiten kann.

Es ist weiterhin nötig, die Übertragung des Verschlüsselungsalgorithmus gegen Erkennen zu sichern und somit das Brechen des Entschlüsselungsalgorithmus weiter zu erschweren. Dies beruht auf der einfachen Tatsache, daß ein Verschlüsselungsalgorithmus, welcher unbekannt ist, wesentlich schwerer zu brechen ist als ein bekannter. Dies ist ebenfalls nötig, damit nicht bekannt ist, welcher Verschlüsselungsalgorithmus zur Verschlüsselung welcher Informationen eingesetzt wird.

5

Es besteht also die Notwendigkeit, ein Verfahren zu finden, mit dem es möglich ist, Verschlüsselungsalgorithmen zu verteilen und die Übertragung dieser gegen Erkunden zu schützen.

10

Weiterhin ist es notwendig, daß es selbst dem Besitzer eines Entschlüsselungsgerätes nicht möglich ist, das Entschlüsselungsverfahren weiterzugeben und damit die Erkundung des Verschlüsselungsalgorithmus zu ermöglichen.

15

Es ist ein Spezialprozessor als Teil dieses Verfahrens zu schaffen, der die Verteilung sowie den Schutz der Entschlüsselungsalgorithmen vor Weitergabe preiswert und sicher realisiert.

Erfindungsgemäß wird diese Aufgabe durch die im Patentanspruch 1 und Patenanspruch 2 angegebenen Merkmale gelöst.

20

Die Erfindung wird nachstehend anhand der Figur 1, die die Entschlüsselungseinrichtung von Entschlüsselungsalgorithmen zeigt und dem Verfahren zur Durchführung der Ver- und Entschlüsselung von digitalen Informationen, dargestellt.

25

Die in Figur 1 dargestellte Entschlüsselungseinrichtung von Entschlüsselungsalgorithmen wird zur Verdeutlichung anhand eines Einsatzes in

mehreren Personalcomputern gezeigt, wobei digitale Informationen an ausgewählte Besitzer von Entschlüsselungseinrichtungen gesandt werden.

Dabei besteht die dargestellte Entschlüsselungseinrichtung aus einem -integrierten Schaltkreis-1, dem ein -Zentralprozessor CPU-2, ein -interner nichtauslesbarer flüchtiger Speicher mit wahlfreiem Zugriff RAM-3 als Arbeitsspeicher und ein -interner nichtauslesbarer nichtflüchtiger Speicher mit wahlfreiem Zugriff ROM-4, in welchem ein interner nichtauslesbarer Entschlüsselungsalgorithmus (EI) gespeichert ist, und ein Interface 5 zugeordnet sind, welches zwischen dem - Zentralprozessor CPU-2 und dem Personalcomputer 6 angeordnet ist und mit dem Personalcomputer 6 mit dem Datenpfad a verbunden ist, und teilweise in einem integrierten Schaltkreis integriert ist.

Das Verfahren zur Durchführung der Übertragung des Entschlüsselungsalgoritmus wird anhand der Figur 1 gezeigt, indem die Entschlüsselungseinrichtung in mehreren Personalcomputern eingesetzt ist, wobei digitale Informationen an ausgewählte Besitzer von Entschlüsselungseinrichtungen gesandt werden.

Die Übertragung eines Entschlüsselungsalgoritmus an eine Entschlüsselungseinrichtung ist wie folgt:

Der Verteiler wählt einen Verschlüsselungsalgoritmus VE. Dieser sei zum Verschlüsseln der später übertragenen Informationen gedacht. Dieser Verschlüsselungsalgoritmus soll geheim gehalten werden und muß weiterhin sicher genug sein, um Sicherheit bei der Verschlüsselung von Nachrichten zu bieten. Dafür würden sich z. B. verschiedene Abarten des DES (z. B. mit verschiedenen S-Boxen) oder andere Verschlüsselungsverfahren eignen.

Nun wird der zum Verschlüsselungsalgoritmus VE passende Entschlüsselungsalgoritmus EE zum unleserlichen Algoritmus EEV verschlüsselt.

Nun kann jeder Benutzer einer Entschlüsselungseinrichtung, der einen Entschlüsselungsalgorithmus erhalten will, sich bei der Verteilerstelle melden. Dies kann z. B. verbal (auch über Telefon), schriftlich oder elektronisch erfolgen. Anhand der öffentlichen Seriennummer der Entschlüsselungseinrichtung muß er sich identifizieren. Da diese Seriennummer nur einmal vergeben wurde, ist eine eindeutige Identifikation der Entschlüsselungseinrichtung möglich. Die Verteilungsstelle kann nun darüber entscheiden, ob der Empfänger berechtigt ist, den Entschlüsselungsalgorithmus zu empfangen. Das kann auch von einer Bezahlung abhängen.

10 Wenn dies geklärt ist, wird der verschlüsselte Entschlüsselungsalgorithmus zum Benutzer der Entschlüsselungseinrichtung übertragen und dort in der Entschlüsselungseinrichtung zum Algorithmus EE entschlüsselt. Damit ist es dann möglich, Nachrichten, die mit dem Verschlüsselungsalgorithmus VE verschlüsselt wurden, zu entschlüsseln.

15 Dies soll nun an einem Ausführungsbeispiel dargestellt werden.

Als Beispiel sei der Empfang eines Entschlüsselungsalgorithmus durch den Besitzer der Entschlüsselungseinrichtung mit der Seriennummer SN=1 erläutert.

20 Die Erzeugung des an die Entschlüsselungseinrichtung mit der Seriennummer SN=1 zu übertragenden verschlüsselten Entschlüsselungsalgorithmus erfolgt folgendermaßen:

Der Verteiler der Nachrichten wählt einen Verschlüsselungsalgorithmus VE, welcher dann zur Verschlüsselung der später zu übertragenden Nachricht genutzt werden soll. Dieser Verschlüsselungsalgorithmus wird nie öffentlich zugänglich, sondern nur in verschlüsselter Form übertragen.

25 Der Hersteller der Entschlüsselungseinrichtung (die Verteilerstelle der Entschlüsselungsalgorithmen und Nachrichten) verfügt über die internen

Entschlüsselungsalgorithmen EI und auch die zugehörigen Verschlüsselungsalgorithmen EIU aller Entschlüsselungseinrichtungen. Diese sind in einer Datenbank beim Hersteller oder auch beim Verteiler gespeichert.

Es sei EI1A, der nur dem Hersteller der Entschlüsselungseinrichtung bekannte interne Entschlüsselungsalgorithmus EI der Entschlüsselungseinrichtung mit der internen Seriennummer SN=1. Weiterhin sei EI1UA, der ebenfalls nur dem Hersteller der Entschlüsselungseinrichtung bekannte Verschlüsselungsalgorithmus, passend zu EI1X.

Nun wird der, der Entschlüsselungseinrichtung zu übertragende Entschlüsselungsalgorithmus EE verschlüsselt. Dies erfolgt in der Art, daß der Entschlüsselungsalgorithmus EE mit dem zum internen Entschlüsselungsalgorithmus EI passenden Verschlüsselungsalgorithmus EIU zum unleserlichen Algorithmus EEV nach folgender Formel verschlüsselt wird:

$$\text{EEV} := \text{EI1U(EE)}.$$

Dieser verschlüsselte Algorithmus EEV wird der Entschlüsselungseinrichtung mit der Seriennummer SN=1 übertragen.

Dies kann z. B. verbal (auch über Telefon), schriftlich oder elektronisch erfolgen.

Der übermittelte Algorithmus ist relativ kurz. Damit ist ein Knacken des internen Entschlüsselungsalgorithmus der Entschlüsselungseinrichtung EI schwer möglich. Wie oben gezeigt, müssen für ein Brechen der Verschlüsselung viele Plain- und Ciphertexte vorhanden sein, um erfolgsversprechende Knackalgorithmen verwenden zu können. Dies ist aber in diesem Fall wegen der Kürze des übermittelten verschlüsselten Entschlüsselungsalgorithmus EEV nicht möglich.

Nun wird beim Empfänger das Entschlüsselungsgerät funktionstüchtig gemacht.

Der Ablauf nach dem Einschalten der Versorgungsspannung oder nach einer Unterbrechung der Abarbeitung ist folgender:

Der -Zentralprozessor CPU-2 führt mit dem -internen nichtauslesbaren nichtflüchtigen Speicher mit wahlfreiem Zugriff ROM-4 und dem -internen nichtauslesbaren flüchtigen Speicher mit wahlfreiem Zugriff RAM-3 einen Selbsttest durch. Dies könnte z. B. durch eine Prüfsummenbildung geschehen.

Nun erfolgt das Einlesen des verschlüsselten Entschlüsselungsalgorithmus EEV in die Entschlüsselungseinrichtung über das Interface 5. Der Entschlüsselungsalgorithmus wurde vorher in verschlüsselter Form vom Benutzer der Entschlüsselungseinrichtung eingegeben oder in anderer Form eingelesen.

Als nächstes wird mit Hilfe des im -internen nichtauslesbaren nichtflüchtigen Speicher mit wahlfreiem Zugriff ROM-4 gespeicherten Entschlüsselungsalgorithmus EI der verschlüsselt vorliegende Entschlüsselungsalgorithmus EEV mit dem internen Entschlüsselungsverfahren EI entschlüsselt. Dies geschieht in der Weise, daß der -Zentralprozessor CPU-2, die im -internen nichtauslesbaren nichtflüchtigen Speicher mit wahlfreiem Zugriff ROM-4 gespeicherte Entschlüsselungseinrichtung, in den Personalcomputer 6 eingegeben werden, Anweisungen des Entschlüsselungsalgorithmus EI ausführt und den verschlüsselten Entschlüsselungsalgorithmus EEV folgendermaßen entschlüsselt:

$$\text{EE} := \text{EI1(EEV)}.$$

Bei diesem Verfahren entsteht wieder, da der interne Entschlüsselungsalgorithmus EI1 mit dem Verschlüsselungsalgorithmus EIU1 zusammenpaßt, mit dem der Entschlüsselungsalgorithmus EE verschlüsselt wurde, der ursprüngliche Entschlüsselungsalgorithmus EE.

Dieser wird im -internen nichtauslesbaren flüchtigen Speicher mit wahlfreiem Zugriff RAM-3 abgespeichert und ist somit nicht von außen erkundbar. Damit ist es nicht möglich, den Entschlüsselungsalgorithmus weiterzugeben, da er in verschlüsselter Form wertlos ist und in unverschlüsselter Form nicht vorliegt.

- 5 Nun ist die Entschlüsselungseinrichtung einsatzbereit.

Die Entschlüsselung einer verschlüsselten Nachricht NV, die z. B. verbal (auch über Telefon), schriftlich oder elektronisch übertragen wurde, in der Entschlüsselungseinrichtung mit der Seriennummer SN=1 erfolgt nun folgendermaßen:

- 10 Die CPU lädt über das Interface 5 den Schlüssel K und die Nachricht NV. Dieser Schlüssel muß auf einem sicheren, Dritten nichtzugänglichen Weg übertragen werden, dies kann auch durch Verschlüsselung geschehen.

Dann wird die Nachricht von dem -Zentralprozessor CPU-2 mit dem Entschlüsselungsalgorithmus EE unter Nutzung des Schlüssels K entschlüsselt:

15  $NE := EE(NV, K)$ .

Danach wird die entschlüsselte Information NE von dem -Zentralprozessor CPU-2 über das Interface 5 ausgegeben und steht dem Empfänger zur Verfügung.

- 20 Es ist somit möglich, Informationen mit verschiedenen Verschlüsselungsalgorithmen zu verschlüsseln und mit verschiedenen Entschlüsselungseinrichtungen zu entschlüsseln, ohne daß der Entschlüsselungsalgorithmus bekannt gemacht werden muß oder vorher schon in der Entschlüsselungseinrichtung vorliegt.

Weiterhin ist der übertragene Entschlüsselungsalgorithmus weder weitergebar oder erkundbar, da er individuell für jedes Entschlüsselungsgerät verschlüsselt

übertragen wird und dort nichtauslesbar gespeichert und nur zum internen Gebrauch des Entschlüsselungsgerätes mit der entsprechenden Seriennummer verfügbar ist.

**Verwendete Bezugszeichen**

- 1 -integrierter Schaltkreis-
- 2 -Zentralprozessor CPU-
- 3 -interner nichtauslesbarer flüchtiger Speicher mit wahlfreiem Zugriff RAM-
- 5    4 -interner nichtauslesbarer nichtflüchtiger Speicher mit wahlfreiem  
      Zugriff ROM-
- 5    Interface
- 6    Personalcomputer
- a    Datenpfad

**Verwendete Abkürzungen**

CPU = Zentralprozessor

DEA = data encryption standard

EI = Entschlüsselungsalgorismus intern

5 EI1 = Entschlüsselungsalgorismus intern für die Entschlüsselungseinrichtung mit der Seriennummer SN=1

EIU = zum internen Entschlüsselungsalgorismus EI passender Verschlüsselungsalgorismus

10 EI1U = zum internen Entschlüsselungsalgorismus EI1 passender Verschlüsselungsalgorismus für die Entschlüsselungseinrichtung mit der Seriennummer SN=1

EE = Entschlüsselungsalgorismus zur Verschlüsselung von Nachrichten

15 EEV = verschlüsselter Entschlüsselungsalgorismus zur Übertragung

NE = nichtverschlüsselte oder entschlüsselte Nachricht

NV = verschlüsselte Nachricht

Schlüssel K = Schlüssel zur Entschlüsselung von Nachrichten

20 VE = Verschlüsselungsalgorismus beim Verteiler der Informationen zur Verschlüsselung der digitalen Informationen passend zu EE

(:=) = ergibt sich aus

## Patentansprüche

1. Entschlüsselungseinrichtungen von Entschlüsselungsalgorithmen, dadurch gekennzeichnet, daß vom Verteiler des Entschlüsselungsalgorithms dieser mit einem Verschlüsselungsalgorithmus (EIU) verschlüsselt wird, welcher dem Entschlüsselungsalgorithmus (EI) entspricht, der in der jeweiligen empfangenden Entschlüsselungseinheit intern vorhanden ist, daß der Entschlüsselungsalgorithmus (EI) der Öffentlichkeit nicht zugänglich und auch nicht erkundbar ist, der Nutzer der Entschlüsselungseinrichtung den verschlüsselten Entschlüsselungsalgorithmus in der Entschlüsselungseinrichtung eingibt und dieser innerhalb der Entschlüsselungseinrichtung entschlüsselt wird, wobei die Entschlüsselungseinrichtung aus einem -integrierten Schaltkreis-(1), dem ein -Zentralprozessor CPU-(2), ein -interner nichtauslesbarer flüchtiger Speicher mit wahlfreiem Zugriff RAM-(3) als Arbeitsspeicher und ein -interner nichtauslesbarer nichtflüchtiger Speicher mit wahlfreiem Zugriff ROM-(4) und einem Interface (5) zugeordnet sind, indem sich jede Entschlüsselungseinrichtung von jeder weiteren unterscheidet durch den Inhalt des -internen nichtflüchtigen Speichers mit wahlfreiem Zugriff ROM-(4) und teilweise in einem -integrierten Schaltkreis-(1) integriert ist und daß das Interface (5) zwischen dem -Zentralprozessor CPU-(2) und dem Personalcomputer (6) angeordnet ist und mit dem -Zentralprozessor CPU-(2) mit dem Datenpfad (a) verbunden sind.

2. Entschlüsselungseinrichtung von Entschlüsselungsalgorithmen und Verfahren zur Durchführung der Ver- und Entschlüsselung derselben dadurch gekennzeichnet, daß im

## 1. Schritt

vom Verteiler der Entschlüsselungsalgorithmen diese mit einem, nur dem Hersteller der Entschlüsselungseinrichtung bekannten Verschlüsselungsalgorithmus (EIU) (welcher dem Entschlüsselungsalgorithmus (EI) in der Entschlüsselungseinheit entspricht, wie folgt verschlüsselt werden:

EEV := EIU(EE)

und dieser verschlüsselte Algorithmus (EEV) der Entschlüsselungseinrichtung übertragen wird, wonach die Entschlüsselungseinrichtung, mit dem -Zentralprozessor CPU-(2) mit dem -internen nichtauslesbaren nichtflüchtigen Speicher mit wahlfreiem Zugriff ROM-(4) einen Selbsttest durchführt, und das Einlesen des verschlüsselten Entschlüsselungsalgorithmus (EEV) in das Entschlüsselungsgerät über das Interface (5) erfolgt und nun mit Hilfe des im -internen nichtauslesbaren nichtflüchtigen Speicher mit wahlfreiem Zugriff ROM-(4) gespeicherten Entschlüsselungsalgorithmus (EI) der verschlüsselt vorliegende Entschlüsselungsalgorithmus (EEV) mit dem internen Entschlüsselungsverfahren (EI) entschlüsselt nach

EE := EI(EEV)

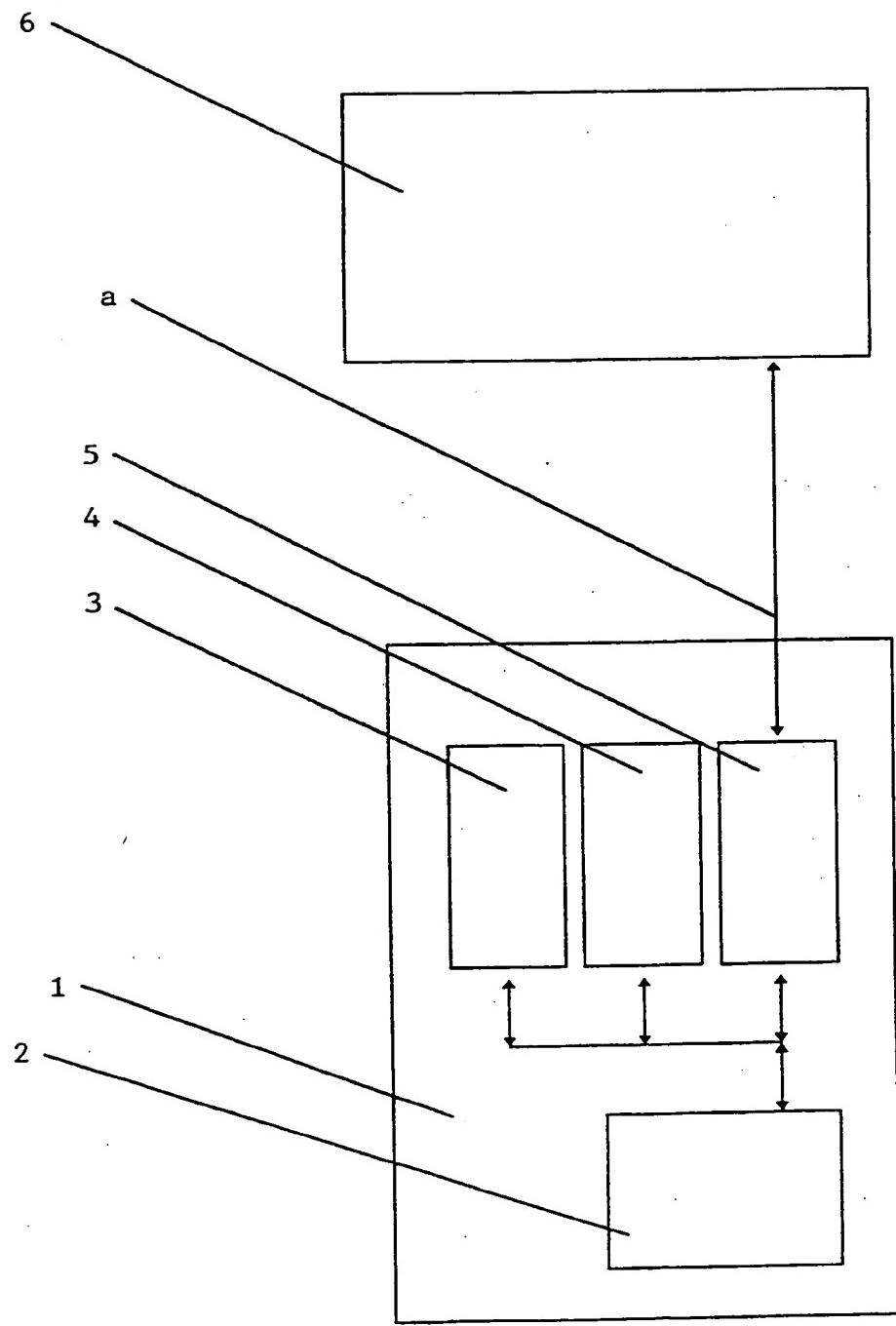
wird, wobei bei diesem Verfahren wieder der ursprüngliche Entschlüsselungsalgorithmus (EE) entsteht, welcher im -internen nichtauslesbaren flüchtigen Speicher mit wahlfreiem Zugriff RAM-(3) abgespeichert, und somit nicht von außen erkundbar ist, womit die Entschlüsselungseinrichtung mit dem Entschlüsselungsalgorithmus (EE) einsatzbereit ist und die Entschlüsselung einer Nachricht (NV) folgendermaßen erfolgt, daß die CPU über das Interface (5) den Schlüssel (K), welcher über einen sicheren Übertragungsweg, z. B. Verschlüsselung, übertragen werden muß, und die Nachricht (NV) lädt und die Nachricht von dem -Zentralprozessor CPU-(2) mit dem Entschlüsselungsalgorithmus (EE) unter Nutzung des Schlüssels (K) entschlüsselt wird, nach

NE := EE(NV, K)

und die entschlüsselte Information (NE) von dem -Zentralprozessor CPU-(2) über das Interface (5) ausgegeben wird und dem Empfänger zur Verfügung steht.

1 / 1

FIGUR 1



## INTERNATIONAL SEARCH REPORT

Int'l Application No  
PCT/DE 95/00733

A. CLASSIFICATION OF SUBJECT MATTER  
IPC 6 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP,A,0 033 014 (LICENTIA) 5 August 1981 see page 2, line 25 - page 4, line 18 ---	1,2
Y	FR,A,2 681 165 (GEMPLUS) 12 March 1993 see page 1, line 12 - line 23 see page 2, line 6 - line 9 see page 6, line 16 - page 7, line 29 see page 10, line 7 - line 18 ---	1,2
Y	PATENT ABSTRACTS OF JAPAN vol. 7, no. 186 (E-193) 30 May 1983 & JP,A,58 090 849 (NIPPON DENKI) 30 May 1983 see abstract ---	2

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

\* Special categories of cited documents :

- \*A\* document defining the general state of the art which is not considered to be of particular relevance
- \*E\* earlier document but published on or after the international filing date
- \*L\* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \*O\* document referring to an oral disclosure, use, exhibition or other means
- \*P\* document published prior to the international filing date but later than the priority date claimed

- \*T\* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- \*X\* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- \*Y\* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- \*&\* document member of the same patent family

Date of the actual completion of the international search

20 September 1995

Date of mailing of the international search report

- 9. 10. 95

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patendaan 2  
NL - 2280 HV Rijswijk  
Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+ 31-70) 340-3016

Authorized officer

Holper, G

## INTERNATIONAL SEARCH REPORT

International Application No  
PCT/DE 95/00733

## C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	FR,A,2 608 338 (ELECTRONIQUE SERGE DASSAULT) 17 June 1988 see page 2, line 21 - line 27 see page 3, line 21 - page 4, line 34 see page 8, line 1 - page 9, line 28 -----	1,2

**INTERNATIONAL SEARCH REPORT**

Information on patent family members

International Application No  
PCT/DE 95/00733

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A-0033014	05-08-81	DE-A- 3003998 US-A- 4484025	24-09-81 20-11-84
FR-A-2681165	12-03-93	NONE	
FR-A-2608338	17-06-88	NONE	

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen  
PCT/DE 95/00733

**A. KLASIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**  
**IPK 6 H04L9/08**

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationsymbole)  
**IPK 6 H04L**

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	EP,A,0 033 014 (LICENTIA) 5. August 1981 siehe Seite 2, Zeile 25 - Seite 4, Zeile 18 ---	1,2
Y	FR,A,2 681 165 (GEMPLUS) 12. März 1993 siehe Seite 1, Zeile 12 - Zeile 23 siehe Seite 2, Zeile 6 - Zeile 9 siehe Seite 6, Zeile 16 - Seite 7, Zeile 29 siehe Seite 10, Zeile 7 - Zeile 18 ---	1,2
Y	PATENT ABSTRACTS OF JAPAN vol. 7, no. 186 (E-193) 30. Mai 1983 & JP,A,58 090 849 (NIPPON DENKI) 30. Mai 1983 siehe Zusammenfassung ---	2 -/--

Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

- \* Besondere Kategorien von angegebenen Veröffentlichungen :
- \*' A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
- \*' E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
- \*' L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
- \*' O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
- \*' P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

Siehe Anhang Patentfamilie

- \*' T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
- \*' X" Veröffentlichung von besonderer Bedeutung, die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erforderlicher Tätigkeit beruhend betrachtet werden
- \*' Y" Veröffentlichung von besonderer Bedeutung, die beanspruchte Erfindung kann nicht als auf erforderlicher Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
- \*' &" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

Absendedatum des internationalen Recherchenberichts

20. September 1995

~ 9. 10. 95

Name und Postanschrift der Internationale Recherchenbehörde  
Europäisches Patentamt, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+ 31-70) 340-2040, Tx. 31 651 cpo nl,  
Fax (+ 31-70) 340-3016

Bevollmächtigter Bediensteter

Holper, G

## INTERNATIONALER RECHERCHENBERICHT

Int. ionales Aktenzeichen  
PCT/DE 95/00733

## C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	FR,A,2 608 338 (ELECTRONIQUE SERGE DASSAULT) 17. Juni 1988 siehe Seite 2, Zeile 21 - Zeile 27 siehe Seite 3, Zeile 21 - Seite 4, Zeile 34 siehe Seite 8, Zeile 1 - Seite 9, Zeile 28 -----	1,2
2		

**INTERNATIONALER RECHERCHENBERICHT**

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/DE 95/00733

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP-A-0033014	05-08-81	DE-A- 3003998 US-A- 4484025	24-09-81 20-11-84
FR-A-2681165	12-03-93	KEINE	
FR-A-2608338	17-06-88	KEINE	